Subject: INFO-HAMS Digest V89 #922
To: INFO-HAMS@WSMR-SIMTEL20.ARMY.MIL

INFO-HAMS Digest Wed, 22 Nov 89 Volume 89 : Issue 922

Today's Topics:
A mobile vhf kilowatt
Military aircraft callsigns...Eugen
Military aircraft callsigns...Eugene Balinski (2 msgs)
military call signs.....etc.
Scanners/freedom to listen/

Date: 22 Nov 89 23:55:09 GMT
From: unsvax!arrakis.nevada.edu!storkus@uunet.uu.net (Mike Storke)
Subject: A mobile vhf kilowatt

The Metron MA-1000B is an HF linear amplifier! I haven't seen any kilowatts out for a while, but you might want to try some people, esp. Henry Radio in Los Angeles. They advertise in all the ham magazines, and I believe they always say they have any amplifier for any application (or something to that effect). Hope this helps some. 73's,
****
Mike P. Storke, N7MSD @ University Nevada/Las Vegas-only a student, sorry :-)
Inet: storkus@arrakis.nevada.edu Packet: KF7TI @ LAS:K7WS-1 or ANGEL:K7WS-2
Snailmail: Box 462 Las Vegas, NV 89119 Sorry, what I say comes from my fingers.
"Pascal: The Handcuff of the Programmer"-ME! I WANT MY C!!!!!!!!!!!!!!!!!!!!

Date: 22 Nov 89 20:31:01 GMT
From: vsi1!daver!lynx!neal@apple.com (Neal Woodall)
Subject: Military aircraft callsigns...Eugen

In article <30500290@ux1.cso.uiuc.edu> phil@ux1.cso.uiuc.edu writes:

>>...In that sense ECPA is a correction of an omission. If the authors
>> of the CommAct had anticipated that cult, the CommAct provisions you
>>cite as permission would not likely exist.

>This depends on WHO writes it and WHEN. If *I* were to write it today, it
>would probably be just about the same as it is, except that there would be
>EXPLICIT references to requiring the use of scrambling and encryption for
>secret communications, and ensuring no more secrecy of communication than
>the scrambling or encryption itself can assure.

I agree with Phil.....the issue in this guise seems to boil down to one of responsibility. Some people seem to think that it is a good idea to

write laws that make THEIR communications security the responsibility of OTHER PEOPLE, and then depend fully on the law to provide the security. IMHO, a very foolish set of assumptions. My opinion is that an individual should be responsible for his/her own security.....

People in general need to take responsibility for their own actions and security; too often people tend to try and place the responsiblity for their actions and omissions on other people. This is childish and immature, just as it is childish to depend upon the "good intentions" of others for your communications security. If you feel that you need to communicate "private info", the take steps to keep that info private.

Neal

Date: 22 Nov 89 20:54:37 GMT
From: vsi1!daver!lynx!neal@apple.com (Neal Woodall)
Subject: Military aircraft callsigns...Eugene Balinski

In article <1071@east.East.Sun.COM> Jim Vienneau writes:

>Can we pleeeease take this discussion to somewhere else? Alt.flame perhaps?
>This discussion is going nowhere fast and taking up lots of bandwidth doing
>it!

Sorry, Jim, but I think that this discussion is relevant....the flames are being kept to a minimum, and this is a discussion of the legal/"moral" aspects of radio monitoring.

Neal

Date: 22 Nov 89 20:50:04 GMT
From: vsi1!daver!lynx!neal@apple.com (Neal Woodall)
Subject: Military aircraft callsigns...Eugene Balinski

Jim Grubs writes:
>> From: neal@lynx.uucp (Neal Woodall)

>>I would like to see you try to tell the Soviet intelligence people to
>>stop listening to SAC because it is "not OK" for them to do so!

>>When you say it is "not OK", do you mean in a legal or moral sense? If

>Moral.

Then lets discuss this "moral"....come on, Jim....I want to have a discussion on why you think that there is some kind or "moral prohibition" against listening to (ie, receiving, demodulating) signals that are sent "in the clear", so that the sender knows the situation and has no reasonable expectation of privacy.

>> What a bunch of B.S.! If you want security, then encrypt! If your idea of
>> "security" is to rely on a law that is practically unenforcable, then you
>> are very confused.

>As a practical matter, it is necessary. It should NOT be necessary. To return
>to the ubiquitous highway/automobile analogy, it is illegal to strip a car in
>a mall parking lot, even if the owner forgot to lock it. Finding an unlocked
>car does not make it or its contents public property.

I am glad that you at least agree that it is necessary to encrypt as a "practical matter" of comsec....hey Jim, the world is NOT a perfect place. You cannot depend on others to do what you expect! In a perfect world, there would be no evil, and lots of security precautions would not be necessary.

So you equate reception and demodualtion or a signal with "stripping" a car. HAH! The radio waves are passing through MY home, MY body.....if someone dumps a bunch of stuff out in public, he has no reasonable expectaion that people will not observe and pick through his stuff. Look, the Supreme Court recently ruled that an individual has no reasonable expectaton of privacy when he throws something away (ie, puts it out in a publically accessible place....the decision that lets cops rummage through trash for evidence). When someone broadcasts a radio signal, he is putting it "out in the open" ....he has no reasonable expectation of privacy!

It would be more strictly analogous to think of an ENCRYPTED signal as being "a locked car." Of course, the ECPA notwithstanding, I think that a person still has a right to try and "demodulate and decrypt" and encrypted signal. I think of it like this: If I own a piece of property, and someone dumps a locked safe onto that property without my permission, then I am going to sieze that safe and attempt to open it.

Neal

Date: 22 Nov 89 20:20:38 GMT
From: vsi1!daver!lynx!neal@apple.com (Neal Woodall)
Subject: military call signs.....etc.

In article <8911212358.AA17672@ti.com> DUBE TODD writes:

>....If any "in-the-clear" radio transmissions are subject to intercept and
>disposition as the interceptor sees fit, then we should get concerned about
>our use of cordless phones. Anyone can park in front of your home and
>receive/record all your personal conversation that you care to "dump" into
>the public domain and do whatever he/she pleases with it; possibly resulting
>in some embarrassment to you and your family. As someone mentioned, it's
>like overhearing a conversation in any public gathering. We can't have it
>both ways.   Think about it.

Look, Mr. Todd....I don't fully understand your position here, but I am
going to let you in on a little secret.....

If you have not already taken precautions to avoid saying anything over a
cordless phone that you don't want others to hear, then you are a fool.

You say we should "get concerned" about our use of cordless phones, well I
think anyone who has not been concerned about their use of cordless phones
from day one is a loser....when you say that "...anyone can park in front of
your home and recieve/record all your personal conversation....", you are
100% correct!! Thus, you better by VERY careful what you say on a cordless
phone....

First, the philosophical aspects: I do not advocate the reception of signals
with the intent of using any information gained thus to victimize or harass
individuals or organizations. I do, however, think that it is foolish to
write laws that try to limit my legal right to receive E-M radiation that
is passing through my home, my body, etc. To me, radio monitoring is a very
interesting and enjoyable hobby. Just as I have a right to listen to any
sound waves that impinge upon my ears, I believe that I have a right to
receive and demodulate radio waves that impinge upon my body. Further, a
person who wants "privacy" in his/her communication should take reasonable
precautions to ensure that privacy....anyone who depends for his/her
communications security on a law or the good intentions of other people
is, IMHO, a naive fool.

People are just going to have to learn that when they use ANY system that

broadcasts radio waves, their communication is subject to being received by anyone who cares to set up a reciever. Laws and "moral prohibitions" will not stop people who are intent on receiving radio waves....if it is technically possible, then people will do it.

I ALWAYS operate under the principle and assumption that ANY type of communication that is being sent over some kind of radio link is subject to reception by un-intended individuals.....I take precautions to encode or encrypt what I consider to be "sensitive information". As for cordless phones, I KNOW better than to use them for private communications!

Second, the practical aspects: the 46/49 MHz frequencies used by cordless phones are readily received by common scanners, AND are used by the "kiddie talkies" that you can buy in any department store for about 20 bucks. No person who uses these frequencies while broadcasting in the clear has any reasonable expectaton of privacy. As to the role of the ECPA in the monitoring of the 46/49 MHz cordless band...there is none! The ECPA does NOT prohibit the reception and demodulation by ANYONE of ANY signal in this band! In fact, there is SPECIFIC LANGUAGE in the ECPA that ALLOWS these bands to be monitored by ANYONE!

So, Mr. Todd, I hope that next time you start to discuss "private info" over your cordless phone, you will stop and think twice!

Neal

Date: 22 Nov 89 16:11:27
From: David Waters <David_Waters.M1@smtp.ESL.COM>
Subject: Scanners/freedom to listen/

Scanners/freedom to listen/etc debate
Comments, re: bad guys using scanners: I've asked several police officers while wondering how often they encounter bad guys that use scanners. The best reply was that if they were smart enough to use a scanner to commit a crime, then they probably are smart enough not to commit the crime in the first place. This makes a lot of sense, and seems to be the case in most things. As stated already, any of the information thus far published here and on other BBS systems (concerning VHF/UHF business/public service scanning anyway) is public information, and can be had through numerous "legal" sources, including the FCC itself. Freedom of information, you know?
Also, most police officers welcome the public's help, although madly pursuing calls heard on the scanner in order to "get involved" is not condoned. Several

times I have had the opportunity to assist police simply due to the fact that I was 1) there and 2) aware (via a scanner) of what they were after. I never do anything that puts either 1) them or 2) me, in jeopardy. I think this is what most citizens would do anyway. As also stated previously, the police officers noted to me that they are very well aware of the fact that people are listening and that most are hobbyists like myself. They do not consider it eavesdropping, since they have secure communications available if necessary.
Thanks for the opportunity to throw MY 2 cents worth in!

David Waters, WA6AWZ
Internet: David_Waters.M1@smtp.ESL.COM

End of INFO-HAMS Digest V89 Issue #922
****